UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/671,941	09/27/2000	Steven R. Tugenberg	GE04609	6202

22863	7590	10/10/2003

MOTOROLA, INC.
CORPORATE LAW DEPARTMENT - #56-238
3102 NORTH 56TH STREET
PHOENIX, AZ 85018

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 10/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**
Office Action Summary	09/671,941	TUGENBERG ET AL.
	Examiner	**Art Unit**	
	Firmin Backer	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 August 2003</u> .

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____ .

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)		4)☐ Interview Summary (PTO-413) Paper No(s). _____ .
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)		5)☐ Notice of Informal Patent Application (PTO-152)
3)☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .		6)☐ Other: .

Response to Amendment

This is in response to an amendment file on August 14th, 2003 for letter for patent filed

on September 27th, 2000 in which claims 1-19 were presented for examination. In the

amendment, claim 1 has been amended, no claim has been canceled, and no claim has been

added. Claims 1-19 remain pending in the letter.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsushima et al

(U.S. Patent Granted Pub. 2002/0161722).

3.   As per claim 1, 12, Matsushima et al teach a method for purchasing items (*a service*

providing apparatus) over a network (*network such as the internet*) using a secure

communication device (*information processing apparatus*) *(see figs 1, 3, page 1 paragraph*

0008, page 3 paragraph 0050, 0059), the secure communication device including a host

processor (*recording medium, 110*), a secure memory (*secure data area, 111*) that includes a

laser-scribed encryption key (*prestore secret key*), and a non-secure memory (*non-secured data*

area, 112) for storing encrypted data *(encrypted personal information such credit card)* wherein

sensitive data *(personal information)* is encrypted within the secure memory using the laser-

scribed encryption key *(prestore secret key)* and stored as encrypted data in the non-secure

memory *(see page 3 paragraph, 0051, 4 paragraph 0063, 0066, 0067, 0070, 0071, 0072, 0074,*

0075), comprising retrieving an encrypted credit card number *(receive from the file serve*

encrypted personal information) and an encrypted secret key *(secret key)* from the non-secure

memory *(nonsecured memory, 112)* *(see fig 2, page 4 paragraph 0072, 0074, 0075, 0081, 0087)*

decrypting *(decrypting)* the encrypted credit card *(credit card information)* and secret key

(media ID) with the laser-scribed encryption key *(prestore secret key)* *(fig 5, page 5 paragraph,*

0083) encrypting *(encrypting)* the credit card number *(personal information)* with a

communication encryption key *(public key)*, the communication encryption key being related to

the secret key *(see paragraph 0086)*; and transferring *(transmitting)* the credit card number, as

encrypted with the communication encryption key, over the network to a destination *(file server*

130) *(see fig 23, page 6 paragraph 0103, 0104)*.

4.   As per claim 2, Matsushima et al teach a method wherein the encrypted data is decrypted

within the secure memory using the laser-scribed encryption key and stored within the secure

memory for use by the host processor *(see page 3 paragraph, 0051, 4 paragraph 0063, 0066,*

0067, 0070, 0071, 0072, 0074, 0075) .

5.   As per claim 3, Matsushima et al teach a method further comprising receiving a personal

identification number (PIN) from a user, decrypting an encrypted PIN with the laser-scribed

encryption key, wherein transferring the encrypted credit card number is performed when the

decrypted PIN and the PIN received from the user compare (*see page 3 paragraph, 0051, 4*

paragraph 0063, 0066, 0067, 0070, 0071, 0072, 0074, 0075).

6.   As per claim 4, 13, Matsushima et al teach a method further comprising receiving

biometric information from a user; decrypting stored biometric information for the user with the

laser-scribed encryption key, performed when the decrypted biometric information compares

with the biometric information received from the user (*see page 3 paragraph, 0051, 4 paragraph*

0063, 0066, 0067, 0070, 0071, 0072, 0074, 0075).

7.   As per claim 5, Matsushima et al teach a method wherein the communication encryption

key is a common session key and wherein the method further comprises the step of generating

the session key using the secret key and information provided by the destination *(see figs 1, 3,*

page 1 paragraph 0008, page 3 paragraph 0050, 0059).

8.   As per claim 6, 14, Matsushima et al teach a method wherein the host processor and

secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a

non-volatile memory *(see figs 1, 3).*

9.   As per claim 7, 15, Matsushima et al teach a method wherein the laser-scribed encryption

key is generated by laserscribing a semiconductor die during fabrication of the secure memory to

create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key
(*see paragraph 0086*).

10.   As per claim 8, 16, Matsushima et al teach a method wherein the laser-scribed encryption
key is generated burning onetime programmable fuses on a semiconductor die during fabrication
of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-
scribed encryption key (*see paragraph 0086*).

11.   As per claim 9, 17, Matsushima et al teach a method wherein the secure memory includes
blocking gates coupled between the laser-scribed encryption key and encryption logic circuitry,
the blocking gates being comprised of logic gates and have a blocking control signal input
preventing access to the laser-scribed encryption key by the encryption logic circuitry.

12.   As per claim 10, 18, Matsushima et al teach a method wherein the laser-scribed
encryption key is unique for each secure memory of a plurality of secure memories of different
processing systems (*see fig 1 and 3*).

13.   As per claim 11, 19, Matsushima et al teach a method wherein the laser-scribed
encryption key is randomly generated for each secure memory of a plurality of secure memories
of different processing systems (*see figs 1 and 3*).

Response to Arguments

14.   Applicant's arguments filed August 14th, 2003 have been fully considered but they are not

persuasive.

Applicant argue that the prior art, Matsushima et al '722 can not be

established as prior art based upon that the fact the reference identifies a related

application which was filed January 14, 2000 that is a continuation in part with no

indication as to what portions of the presently cited reference my have been

originally present or may have been later added. However upon a minimally

review of the earlier application, as suggested by the Applicant, Examiner

conclude that the parent and child application are very similar in scope and the

portion of the reference cite in indeed incorporate in the continuing application.

For instance the parent application disclose an information processing device 102

generally a personal computer, but can also be a device that specializes in internet

access, such as a network computer, an internet device, or internet-accessible TV,

STB, and the file server 103 send and receive data to and from each other via a

communication line. The recording media 101 is generally a semiconductor media

from which the information processing device 102 retrieves information, includes

a secured data area 201, a data area 202, and a media ID 203 that is inside the

secured data area 201 from the recording media 101. The secured data area 201 is

a data area that cannot be accessed without an authentication that the device has

an authority to access the recording media 101. The data area 202 is a data area

that can be accessed even without an authentication between the recording media

101 and the device writing and/or reading data to and/or from the recording

device 101.

The information processing device 102 includes input means 301, encryption

means 302, information sending means 303, information retrieval means 304,

information receiving means 305, and data displaying means 310. The input means 301

includes a mouse and a keyboard for receiving commands from the user. Examples of

user's input include a request for browsing file, user information, a request for sending

user information, and a request for sending media ID. When the encryption means 302

receives user information from the input means 301, the encryption means 302 encrypts

the user information. This encryption utilizes a public key encryption such as the RSA

encryption. In other words, a key for encryption is different from a key for decryption.

Applicant is advised to request a copy of the application in accordance to MPEP

103, in order to analyze the priority document in order to determine if the parent

application teaches the subject matter.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing
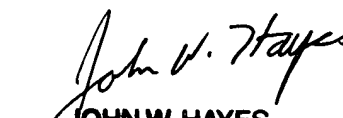
date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The

examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the

organization where this application or proceeding is assigned are (703) 305-7687 for regular

communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is (703) 308-1113.

Firmin Backer
Examiner
Art Unit 3621

October 8, 2003

JOHN W. HAYES
PRIMARY EXAMINER